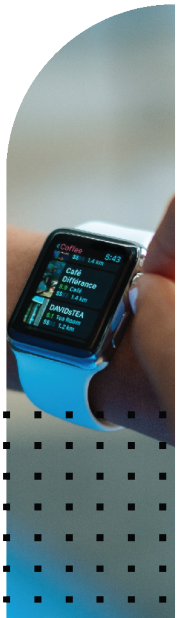
Release Notes

FortiOS 7.0.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 27, 2022
FortiOS 7.0.4 Release Notes
01-704-757204-20220127

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-01-27	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.4 build 0301.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.4 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Changes in CLI

Bug ID	Description
735470	The following settings under `config firewall vip/vip6` are hidden when NAT46/NAT64 is enabled: • `http-redirect` • `http-multiplex` • `max-embryonic-connections` • `http-host` • `http-host` option for `ldb-method`
738151	Previously, SSL certificate options for VIP access proxy configurations contained an option for CA certificates. A configuration using a CA certificate would cause a *ERR_SSL_KEY_USAGE_INCOMPATIBLE* error because it is not a server certificate. Now, the CLI will filter out certificates that do not exist, are a CA certificate, or are not valid. Previous configurations in which SSL certificate options get filtered are upgraded to use default the FORTINET_SSL certificate.

749250	Add setting for IPv4 reachable time (previously only IPv6 was supported).
	`config system interface`
	`  edit <name>`
	`  set reachable-time <integer>`
	`  next`
	`end`
	The IPv4 reachable time is measured in milliseconds (30000 - 3600000, default = 30000).

751346	Allow IPv6 DNS server override to be set when DHCPv6 prefix delegation is enabled.
	`config system interface`
	`  edit <name>`
	`  config ipv6`
	`  set ip6-mode static`
	`  set dhcp6-prefix-delegation enable`
	`  set ip6-dns-server-override enable`
	`  end`
	`  next`
	`end`

753631	Add option to configure H323/RAS direct model traffic.
	`config system settings`
	`  set h323-direct-model {enable | disable}`
	`end`
	The setting is disabled by default (the wide open pinhole will be closed); however when upgrading from an older version, the setting will be enabled to preserve the previous behavior.

Changes in GUI behavior

Bug ID	Description
740767	When registering on FortiCloud, administrative logins using FortiCloud single sign-on are allowed by default.

Changes in default behavior

Bug ID	Description
718290	When using FortiGuard servers for DNS, FortiOS will default to using DNS over TLS (DoT) to secure the DNS traffic. New FortiGuard DNS servers are added as primary and secondary servers.
748811	Accept MTU in ICMP fragmentation needed for ESP packets. In the IPsec phase 2 settings, if `ipv4-df` is enabled, the DF flag in the new IP header is set to the same as the original IP header. If `ipv4-df` is disabled, the DF flag in the new IP header is set to 0.
759012	The default DNS servers have changed, and the default setting is to use DoT and SDNS.

Changes in default values

Bug ID	Description
745999	Change ZebOS and daemons to use a default priority of 1 so a value of 0 is no longer allowed. After upgrading, the old value will be increased by 1 with a maximum value of 65535. The range for the `set priority` option is 1 - 65535.
747175	Change default DDNS update interval from 300 to 0. For FortiGuard DDNS, the default value of 0 is equal to 300 seconds. For third party DDNS servers, the value of 0 means use the update interval assigned by the DDNS server.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
366327	Add `uncompressed/compressed` parameter for `execute backup disk log ftp` command to upload uncompressed log files to an FTP server. An FTP PUT file callback is used to decompress LZ4 log data to text in the memory and send it to the server for storage. • `# execute backup disk alllogs ftp <IP_address> <username> <password> <compressed | uncompressed>` • `# execute backup disk log ftp <IP_address> <username> <password> <log_type> <compressed |uncompressed>`
655389	Add IPv6 options for SSH client in the CLI. `# execute ssh6-options {interface <outgoing_interface> | reset | source6 <source_IPv6_interface> | view-settings}`
675164	Add support for WPA3 encryption on local radios of all FortiWiFi F-series models. These models can now support security modes WPA3-SAE, WPA3-OWE, and WPA3-Enterprise.

691337	Allow a GCP SDN connector to have multiple projects attached to it. Previously, GCP SDN connectors could only be associated with one project, a limit of 256 SDN connectors, and users could only add a maximum 256 projects to the FortiGate. A single GCP SDN connection can now have thousands of projects attached to it.
	Add support for dynamic address filters based on project name and zones:
	`config system sdn-connector`
	`edit <name>`
	`set type gcp`
	`config gcp-project-list`
	`edit <name>`
	`set gcp-zone-list <name_1> <name_2> ... <name_n>`
	`next`
	`end`
	`next`
	`end`
	GUI changes:
	• Add buttons to switch between *Simple* and *Advanced* project configurations. The simple configuration displays a single text field to add one project to the GCP SDN connector.
	• The advanced configuration displays a mutable table for users to add multiple projects to the GCP SDN connectors. Adding projects displays a slide-out pane to specify the project name and zones.
	• A confirmation slide-out pane appears when switching from advanced to simple to warn about projects being deleted from the GCP SDN connector.
	• A tooltip on the GCP SDN connector card shows the list of projects, and the filter list of GCP dynamic addresses shows the project and zones.

Bug ID	Description
696871	Allow SSL VPN web portals to be defined in the ZTNA access proxy settings. The ZTNA access proxy handles the user and device authentication, posture check, and establishes the HTTPS connection between the end user and the access proxy. Then it forwards the user to the web portal where they can use pre-defined bookmarks to access internal and external resources.
711577	Add warnings to inform users when an installed firmware is not signed by Fortinet. The warning message appears in the CLI when the uploaded firmware fails signature validation, and when logging in to the FortiGate from the GUI. Additional messages are added in various places once a user is logged in to the GUI to remind them of the unsigned firmware.
717947	FortiGuard outbreak alerts, which identify outbreaks of security incidents and exploits, are now included as *Security Rating* posture checks. This helps provide information and remediation methods within the *Security Rating* module to protect the network from the exploits and attacks.
718332	In previous DARRP implementation, channel bandwidth was not considered. Now, DARRP will also consider the radio bandwidth in its channel selection, adding support for 40, 80, and 160 MHz channel bandwidth.
720539	Support SMB for ZTNA TCP forwarding.
720687	Add VLAN switch support on FG-20xF.

726974	Support UPN format for the user when adding it to an HTTP header.
	`config web-proxy profile`
	`  edit "AddUPNHeader"`
	`  set log-header-change enable`
	`  config headers`
	`  edit 1`
	`  set name "X-Authenticated-User"`
	`  set content "$user"`
	`  next`
	`  edit 3`
	`  set name "X-Authenticated-UPN"`
	`  **set content "$upn"**`
	`  next`
	`  edit 2`
	`  set name "X-Authenticated-Domain"`
	`  set content "$domain"`
	`  next`
	`  end`
	`  next`
	`end`

728915	Add REST API events log subtype to log POST, PUT, DELETE, and GET REST API requests.
	`config log setting`
	`  set rest-api-set enable`
	`  set rest-api-get enable`
	`end`

Bug ID	Description
730337	Add the following ZTNA enhancements to FortiView and the log view: • Add *FortiView ZTNA Servers* monitor, which includes options to drill down by *Sources*, *Rules*, *Real Servers*, and *Sessions*. • Add context menu shortcuts on the *ZTNA Rules* and *ZTNA Servers* tabs to redirect to the FortiView and log view pages. • Replace *Log & Report* > *ZTNA* page with *Log & Report* > *ZTNA Traffic* page. ZTNA logs now have a traffic type and ZTNA subtype. • Add fields to ZTNA traffic logs.
731720	Add wireless controller syslog profile, which enables APs to send logs to the syslog server configured in the profile.
731721	Add support for advertising vendor specific elements over beacon frames containing information about the FortiAP name, model, and serial number. This allows wireless administrators doing site surveys to easily determine the coverage area of an AP.
732010	When a FortiAP is connected to a switch port with 802.1x authentication enabled, the FortiAP can be configured to act as an 802.1x supplicant to authenticate against the server using EAP-FAST, EAP-TLS, or EAP-PEAP.
735929	Add REST API in both FortiNAC and FortiGate that is used by FortiNAC to send user logon/logoff information to the FortiGate. A new dynamic firewall address type (FortiNAC tag) is added to FortiOS, which is used to store the device IP, FortiNAC firewall tags, and FortiNAC group information sent from FortiNAC via the REST API when user logon/logoff events are registered. The FortiNAC tags connector under *Security Fabric* > *Fabric Connectors* is deprecated. For upgrade support, the FSSO FortiNAC user type can still be configured from the CLI.
738640	Add 100 Mbps transceiver support for FGR-60F.

739145	Federated upgrade for managed FortiSwitches allows a newly authorized FortiSwitch to be upgraded to the latest supported version automatically. The latest compatible FortiSwitch firmware is downloaded from FortiGuard without needing user intervention.
	`config switch-controller managed-switch`
	`edit <id>`
	`set fsw-wan1-peer <interface>`
	`set fsw-wan1-admin enable`
	`set firmware-provision-latest {once | disable}`
	`next`
	`end`
	`config switch-controller global`
	`set firmware-provision-on-authorization {enable | disable}`
	`end`
	If `firmware-provision-on-authorization` is set to `enable`, `firmware-provision-latest` will be set to `once` automatically when the FortiSwitch administrative status (`fsw-wan1-admin`) is enabled.
	When the FortiSwitch connection status becomes authorized or up, a one-time upgrade to the latest compatible firmware version starts if `firmware-provision-latest` is set to `once`.

Bug ID	Description
	A FortiSwitch can connect to multiple VDOMs, and it will be upgraded through any VDOM that it is authorized in.
739170	Add settings on *Network* > *Interfaces* page to configure DSL interfaces and associated DSL settings.
739173	This enhancement improves upon BGP conditional advertisement by accepting multiple conditions to be used together. The conditional route map entries are treated with an AND operator. When the `condition-type` is `exist`: • If the conditional route map matches, then advertised route map will apply. • If the conditional route map does not match, then the advertised route map will not apply. When the `condition-type` is `non-exist`: • If the conditional route map matches, then the advertised route map will not apply. • If the conditional route map not matches, then advertised route map will apply.
739740	Add a map of FortiSwitch model prefixes to full model names, and update the GUI to use these full model names on the *Managed FortiSwitches* page. For example, in previous versions the *Model* displayed for a FortiSwitch would be *FS1D24*, and now it is displayed as *FortiSwitch 1024D*.
739882	Allow configurations pushed from FortiManager to edit tags, FortiClient EMS certificate fingerprints, and FortiClient EMS capabilities. FortiManager sourced changes to the following tables/attributes are allowed: • endpoint.fctems:capabilites • endpoint.fctems:certificate-fingerprint • firewall.address:address of type ems-tag
740525	Add support for multiple DARRP profiles to assign different DARRP settings and optimization schedules to different sets of APs.
740774	Previously, users could be assigned to VLANs dynamically according to the RADIUS attribute `Tunnel-Private-Group-Id` returned from the Access-Accept message. The value can either match a particular VLAN ID or a VLAN interface name. A third option is now added to match based on a VLAN name table defined under the virtual AP.

741715	Add option to allow administrators to enable or disable FFDHE groups for VIP SSL key share.
	`config firewall vip`
	`edit "access-proxy"`
	`set type access-proxy`
	`set ssl-accept-ffdhe-groups {enable | disable}`
	`next`
	`edit "server-load-balance"`
	`set server-load-balance`
	`set ssl-accept-ffdhe-groups {enable | disable}`
	`next`
	`end`

742162	License enforcement on downstream devices by: • Supporting the CSF REST API via a FortiGate Cloud (FGC) tunnel from the root to downstream devices and vice-versa.

Bug ID	Description
	• Restricting create, edit, and delete permissions when accessing devices without a subscription from the FortiGate Cloud portal. • Adding the ability to re-run notifications when switching via the CSF FortiGate chooser dropdown. • Showing read-only access notifications when users switch to a downstream device without a paid subscription from the FortiGate Cloud portal.

742364	Add options to increase flexibility in controlling how the FortiGate's routing engine resolves the BGP route's next hops.
	`config router bgp`
	`  set tag-resolve-mode {disable | preferred | merge}`
	`end`
	The `preferred` option uses a tag match if a BGP route resolution with another route containing the same tag is successful
	The `merge` option merges the tag match with best match if they are using different routes. The results excludes the next hops of tag matches whose interfaces have appeared in best match.

745135	Provide three sizes of internet service databases and an option to choose between full, standard, and mini databases. The FortiGate 30 and 50 series can only configure the mini size.
	`config system global`
	`  set internet-service-database {mini | standard | full}`
	`end`

745240	Add maximal field for each resource in `get system performance status` and improve average value accuracy by rolling over samples immediately when queried. Extend `api/v2/monitor/system/resource/usage` to include new maximum, minimum, and average fields for each resource.

745590	Add user configuration clock skew tolerance for SAML users.
	`config user saml`
	`  edit <name>`
	`  set clock-tolerance <integer>`
	`  next`
	`end`
	The clock skew tolerance is set in seconds (0 - 300, default = 15, 0 = no tolerance).

746496	Optimize broadcast and multicast suppression over SSID tunnel mode across the FortiAP network.
747602	Allow customization of RDP display size (width and height settings) for SSL VPN web mode when creating a new connection or bookmark. Administrators can also specify the display size when pre-configuring bookmarks.
747640	Support Q-in-Q (802.1Q in 802.1Q) for FortiGate-VMs.

Bug ID	Description
749070	The `execute fortitoken-cloud migrate-ftm <license> <vdom>` command allows the migration of FortiToken Mobile users from FortiOS to FortiToken Cloud. The FortiToken Cloud account must be using a time-based subscription license. A request must be made to Fortinet Customer Service to initiate and pre-authorize the transfer. All current active FortiToken Mobile users will be migrated to the FortiToken Cloud license with no changes to the FortiToken Mobile serial number. The FortiOS user or administrator's two-factor setting is automatically converted from `fortitoken` to `fortitoken-cloud`. After migration, end users will be able to authenticate as before without any changes to their FortiToken mobile app.
749895	The `network-import-check` option in BGP can now be configured per prefix, in order to override the setting configured at the global BGP level.

749917	Add option in ZTNA deny policy to display a block notification when a client is blocked instead of silently dropped (default = disable).
	`config firewall proxy-policy`
	`edit <id>`
	`set proxy access-proxy`
	`set block-notification {enable | disable}`
	`next`
	`end`

749981	Allow the AWS SDN connector to use the AWS security token service (STS) API to connect to multiple AWS accounts concurrently. This allows a single AWS SDN connector to retrieve dynamic objects from multiple accounts, instead of needing to create an SDN connector for each account.
	`config system sdn-connector`
	`edit "aws1"`
	`config external-account-list`
	`edit "arn:aws:iam::6*******5494:role/CrossAccountSTS"`
	`set region-list "us-west-1" "us-west-2"`
	`next`
	`edit "arn:aws:iam::9*******1167:role/CrossAccountSTS"`
	`set region-list "us-west-1" "us-west-2"`
	`next`
	`end`
	`next`
	`end`

749982	Support activation of Flex-VMs when connecting to the internet using a web proxy. `# execute vm-license <token> http://user:pass@proxyip:proxyport`
750319	Support UTM scanning and deep inspection for mail protocols SMTP, IMAP, and POP3 in ZTNA TCP forwarding access proxy.
750702	Add support for FQDN and ZTNA TCP forwarding. A wildcard domain name can be in the TCP forwarding access proxy with the `domain` option under the real server settings. When a domain name request arrives, it matches the domain in the request with the configured domain.

Bug ID	Description
	If there is a match, a DNS request is made and the destination of the request is the DNSed IP. If there is no match, a DNS request is made and the DNSed IP is matched with the configured real server's IP.
750902	Introduce real-time FortiView monitors for *Proxy Sources*, *Proxy Destinations*, and all *Proxy Sessions*. Proxy policy sessions are no longer show in *FortiView Policies* and *FortiView Applications*.
751275	Add WebSocket for Security Fabric events. Subscribers to the WebSocket , such as the *Fabric Management* page, will be updated upon new Fabric events and alert users to reload the page.
753409	Support new speed option, media type, and FEC implementation on the following models: FG-110xE, FG-220xE, FG-330xE, FG-340xE, FG-360xE, FG-396xE, and FG-398xE.
756637	When configuring a FortiExtender in LAN extension mode, the addressing mode for the new LAN extension interface can use IPAM to assign an interface address and DHCP server address range.
756638	Add FortiExtender LAN extension to FortiGate VMs running on public clouds.

757948	Add sub-option 5 to DHCP relay daemon to support some DHCP servers that identify the required client subnets.
	`config system interface`
	`edit <interface>`
	`set dhcp-relay-link-selection <class_IP>`
	`next`
	`end`

761397	Add *Process Monitor* page for displaying running processes with their CPU and memory usage levels. Administrators can view a list of running processes, sort and filter them, and select a process to terminate it. Enhancements have been made to the FortiGate Support Tool Chrome extension, including: backend capture support, CSF support, more daemon logging, pre-process CPU and memory charts, crash log support, REST API profiling, organized node logging, and WebSocket messages.
763275	In dynamic port policies, it is now possible to use the hardware vendor as a filter for the device patterns.
764679	Add new entry when dumping the address table information to list the number of octets for the IP type (SNMP).

765322	To improve GUI performance, an option is added to enable loading static GUI artifacts cached in CDN (content delivery network) servers closer to the user rather than from the FortiGate. On failure, the files can fall back to loading from the FortiGate.
	`config system global`
	`set gui-cdn-usage {enable | disable}`
	`end`

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.0.4 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.2
FortiManager	• 7.0.2
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 22
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiSandbox	• 2.3.3 and later, 4.0.0 is recommended

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC
14. FortiNAC
15. FortiVoice
16. FortiDeceptor
17. FortiAI
18. FortiTester

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.4. When Security Fabric is enabled in FortiOS 7.0.4, all FortiGate devices must be running FortiOS 7.0.4.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1 and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE) will support strong ciphers in the future release of version 5.4.3.

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

   Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2tp.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`edit "test-vip46-1"`
`set extip 10.1.100.155`
`set mappedip 2000:172:16:200::55`
`next`
`end`
	`config firewall vip`
	`edit "test-vip46-1"`
	`set extip 10.1.100.150`
	`set nat44 disable`
	`set nat46 enable`
	`set extintf "port24"`
	`set ipv6-mappedip 2000:172:16:200::55`
	`next`
	`end`

`ippool6` object:

Old configuration	New configuration
config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 **set nat46 enable** next end

NAT46 policy:

Old configuration	New configuration
config firewall policy46 edit 1 set srcintf "port24" set dstintf "port17" set srcaddr "all" set dstaddr "test-vip46-1" set action accept set schedule "always" set service "ALL" set logtraffic enable set ippool enable set poolname "test-ippool6-1" next end	config firewall policy edit 2 set srcintf "port24" set dstintf "port17" set action accept **set nat46 enable** set srcaddr "all" set dstaddr "test-vip46-1" set srcaddr6 "all" set dstaddr6 "all" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname6 "test-ippool6-1" next end

`vip64` object

Old configuration	New configuration
config firewall vip64 edit "test-vip64-1" set extip 2000:10:1:100::155 set mappedip 172.16.200.155 next end	config firewall vip6 edit "test-vip64-1" set extip 2000:10:1:100::155 set nat66 disable **set nat64 enable** **set ipv4-mappedip 172.16.200.155** next end

`ippool` object

Old configuration	New configuration
config firewall ippool edit "test-ippool4-1"	config firewall ippool edit "test-ippool4-1"

Old configuration	New configuration
set startip 172.16.201.155 set endip 172.16.201.155 next end	set startip 172.16.201.155 set endip 172.16.201.155 **set nat64 enable** next end

NAT64 policy:

Old configuration	New configuration
config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end	config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept **set nat64 enable** set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end

Product integration and support

The following table lists FortiOS 7.0.4 product integration and support information:

Web browsers	• Microsoft Edge 94 • Mozilla Firefox version 96 • Google Chrome version 97 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0304 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

FortiExtender	• 4.0.0 and later, 7.0.3 is recommended
AV Engine	• 6.00270
IPS Engine	• 7.00105

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 96 Google Chrome version 97
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 96 Google Chrome version 97
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 96 Google Chrome version 97
macOS Monterey 12.0	Apple Safari version 15 Mozilla Firefox version 96 Google Chrome version 97
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.0.4. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
665173	Crash logs are sometimes truncated/incomplete.
723686	The partial fetch handling in the IMAP proxy only detects and scans the first fetched section, which allows threats in subsequent fetched sections to go through the firewall undetected.

Application Control

Bug ID	Description
752569	Per IP shaper under application list does not work as expected for some applications.

Data Leak Prevention

Bug ID	Description
763687	If a filter configured with `set archive enable` matches a HTTP post, the file is not submitted for archiving (unless `full-archive proto` is enabled).

DNS Filter

Bug ID	Description
748227	DNS proxy generated local out rating (FortiGuard category) queries can time out if they are triggered for the same DNS domains with the same source DNS ID.
751759	DNS filter breaks DNS zone transfer because the client socket might close prematurely (in which there is still some data in the user space) if the server side closed the connection.

Endpoint Control

Bug ID	Description
744613	EMS endpoint IP and MAC addresses are not synchronized to the ZTNA tags on the FortiGate.
747303	Some tagged endpoints' registration is lost on the FortiGate.

Explicit Proxy

Bug ID	Description
664380	When configuring explicit proxy with forward server, if `ssl-ssh-profile` is enabled in `proxy-policy`, WAD is unable to correctly learn the destination type correctly, so the destination port is set to 0, but the squid proxy server does not accept the request and returns an error.
747840	When configuring authentication schemes to negotiate and NTLM (mix), Firefox may not show the authentication pop-up with an explicit proxy.
754259	When an explicit proxy policy has a category address as destination address, the FortiGate needs to check if the address is a Google Translate URL for extra rating. This will trigger a keyword match. However, if a web filter profile is not set yet, WAD will crash. The fix will delay the keyword match until a web filter profile is present.
755298	SNI `ssl-exempt` result conflicts with CN `ssl-exempt` result when SNI is an IP.

Firewall

Bug ID	Description
732604	TCP zero window advertisements not occurring in proxy mode and causing premature server disconnects.
739949	In HA vcluster scenario, the *Bytes* counter on the *Firewall Policy* page always shows *0 B* for the secondary while the *Edit Policy* page shows the correct *Total bytes* in the statistics.
746891	Auto-update script sent from FortiOS GUI has a policy ID of zero, which causes FortiManager to be out of synchronization.
747190	When `auto-asic-offload` is enabled in policy, IP-in-IP sessions show as expired while tunnel traffic goes through the FortiGate.
752411	Kernel panic occurs and device reboots due to `pba_map_index overflow`.
752899	Multicast packet is forwarded from non-VWP port to a VWP port.

Bug ID	Description
754240	After a session updates its shaping policy, if the new shaping policy does not configure a per-IP shaper, the session will still use the old per-IP shaper from the previous shaping policy.
767226	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, the `mappedip` is used for the RST packet's source IP instead of the external IP.

FortiView

Bug ID	Description
546312	Application filter does not work when the source is ISDB or unscanned.

GUI

Bug ID	Description
473841	Newly created deny policy incorrectly has logging disabled and can not be enabled when the CSF is enabled.
535794	Policy page should show new name/content for firewall objects after editing them from the tooltip.
663558	When logging in to a VDOM in the GUI with JSConsole, the system event log displays an incorrect IP address.
698435	The *Edit Virtual IP* page should not display *Conflicts with the External IP of another VIP* when changing the source filter setting.
714455	CLI shows EMS tag object in the address select list, but it is not available in the GUI omni select list.
729324	*Managed FortiAPs* and *Managed FortiSwitches* pages keep loading when VDOM administrator has `netgrp` and `wifi` read/write permissions.
730466	The search does not work on the *Policy & Objects* > *Addresses* page if there is a non-EMS address group with an EMS tag (invalid configuration).
730533	On the *Policy & Objects* > *Firewall Policy* page, an unclear error message appears when a user creates a new SSL VPN policy with a web mode portal and a VIP or VIP group is used as the destination address.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP.
738027	The *Device Inventory* widget shows *no results* when there are two *user_info* parameters.
742626	The VDOM dropdown list in the banner should be scrollable.

Bug ID	Description
746239	Unable to create new VIP when there is another VIP with same external IP and mapped IP ranges and different services.
746953	On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry.
748530	A gateway of *0.0.0.0* is not accepted in a policy route.
749451	On the *Network* > *SD-WAN* page, the volume sent/received displayed in the charts does not match the values provided from the REST API when the RX and TX values of `diagnose sys sdwan intf-sla-log` exceed 2^{32}-1.
750490	Firewall policy changes made in the GUI remove the replacement message group in that policy.
751219	*Last Login* in *SSL-VPN* widget is shown as *NaN* on macOS Safari.
751482	cmbdsvr signal 11 crash occurs when a wildcard FQDN is created with a duplicate ID.
752530	Sandbox status is shown as disabled on *FortiGate Cloud* widget when it is connected.
753000	Guest group that expires after first logon displays the duration variable as the *Expires* value. The value is correct if the administrator logs in and goes to *Guest User Management*.
753354	Interface migration wizard does not migrate all references.
753398	httpsd crashes after NGFW policy is deleted.
754539	On the *Policy & Objects* > *Addresses* page, filters applied on the *Details* column do not work.
755239	VIP with *External IP* configured to *0.0.0.0* is not showing in the GUI.
755625	Application control profile cannot be renamed from the GUI.
755893	Sometimes when changing the language from English to another language, the subcategories under the *Dashboard* menu do not change.
756420	On the *Security Fabric* > *Fabric Connectors* page, the connection to FortiManager is shown as down even if the connection is up. **Workaround**: check the status in the CLI using `diagnose fdsm central-mgmt-status`.
757130	After upgrading, the new ACME certificates configured in the GUI are using the staging environment.
757570	*Path already in use* error appears when adding new HTTPS ZTNA API gateway entry (the CLI allows this configuration).
757606	*Failed to retrieve info* error appears when viewing the *Users & Devices* dashboard.
758820	Unable to restore encrypted backup configuration to TFTP server in the GUI.
760863	PPPoE interface is not selectable if interface type is *SSL-VPN Tunnel*.
761615	Unable to see details of Apache.Struts.MPV.Input.Validation.Bypass log.
761658	*Failed to retrieve information* warning appears on secondary node faceplate.

Bug ID	Description
761933	FSSO user login is not sorted correctly by duration on *Firewall Users* widget.
762683	The feature to send an email under *User & Authentication* > *Guest Management* is grayed out.
764744	On the *Network* > *Explicit Proxy* page, the GUI does not support configuring multiple outgoing IP addresses. **Workaround**: use the CLI.
770948	When using NGFW policy-based mode, the *VPN* > *Overlay Controller VPN* option is removed.
772311	On the LDAP server page, when clicking *Browse* beside *Distinguished Name* and then clicking *OK* after viewing the query results, the LDAP server page is missing fields containing the server settings.

HA

Bug ID	Description
701367	In an HA environment with multiple virtual clusters, *System* > *HA* will display statistics for *Uptime*, *Sessions*, and *Throughput* under virtual cluster 1. These statistics are for the entire device. Statistics are not displayed for any other virtual clusters.
711521	When HA failover happens, there is a time difference between the old secondary becoming the new primary and the new primary's HA ID getting updated. If a session is created in between, the session gets a wrong HA ID, which indicates incorrectly that the session's traffic needs to be handled by the new secondary.
729719	When enabling `ha-direct`, some invalid configurations should be reset and hidden.
730770	After a hasync crash, the FGFM process stops sending keepalives.
731570	VDOMs added and deleted on the FGCP secondary device with the REST API are not synchronized between the FGCP cluster.
732201	VDOM restore on an already configured VDOM causes high CPU sometimes on the primary.
738934	No GARP is being sent out on the VWP interface upon HA failover, causing a long failover time.
740933	HA goes out of synchronization when uploading a local certificate.
747270	When the HA secondary device relays logs to the primary device, it may encounter high CPU usage.
750004	The secondary FortiGate shows a DHCP IP was removed due to conflict, but it is not removed on the primary FortiGate.
752892	PPPoE connection gets disconnected during HA failover.
752928	fnbamd uses `ha-mgmt-interface` for certificate related DNS queries when `ha-direct` is enabled.

Bug ID	Description
753295	Configuration pushed from FortiManager does not respect `standalone-config-sync` and is pushed to all cluster members.
754599	SCTP sessions are not fully synchronized between nodes in FGSP.
757494	Unable to add a member to an aggregate interface that is down in a HA cluster.
760562	hasync crashes when the size of hasync statistics packets is invalid.
761581	`Tunnel to Fortimanager is down` log message is generated on the secondary FortiGate unit (without HA management interface).
766842	Long wait and timeout when upgrading FG- 3000D HA cluster due to vluster2 being enabled.

Intrusion Prevention

Bug ID	Description
739272	Users cannot visit websites with an explicit web proxy when the FortiGate enters conserve mode with `fail-open` disabled. Block pages appear with the replacement message, *IPS Sensor Triggered!*.
751027	FortiGate can only collect up to 128 packets when detected by a signature.

IPsec VPN

Bug ID	Description
715671	Traffic is failing on dialup VPN IKEv2 with EAP authentication.
726326, 745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
740475	Traffic cannot be sent out through IPsec VPN tunnel because SA is pushed to the wrong NP6 for platforms where NP6 is standalone. Affected models: FG-2000E and FG-2500E.
740624	FortiOS 7.0 has new design for dialup VPN (no more route tree in the IPsec tunnel), so traffic might not traverse over the dialup IPsec VPN after upgrading from FortiOS 6.4.6 to 7.0.1, 7.0.2, or 7.0.3 if the server replies on the static route over the dynamic tunnel interface to route the traffic back to the client.
743732	If a failure happens during negotiating a shortcut IPsec tunnel, the original tunnel NAT-T setting is reset by mistake.
744598	Tunnel interface MTU settings do not work when `net-device` is enabled in phase 1.
748746	OCVPN is unable to retain `set save-password enable` option.

Bug ID	Description
752947	The hub sometimes allows the IKEv2 IPsec tunnel with a spoke to be established that uses an expired or revoked certificate.
760428	iked crashes due to responder child_sa creation failing in some cases.
762953	When the primary unit synchronizes the dialup `mode-cfg` assigned IP to the secondary unit, the `mode-cfg` IP is not marked as used in the IP pool. After a HA failover to the secondary unit, the new primary will assign the used IP to a new client. This caused a route clash, and the connection keeps getting flushed and re-established.
767945	In a setup with IPsec VPN IKEv2 tunnel on the FortiGate to a Cisco device, the tunnel randomly disconnects after updating to 7.0.2 when there is a CMDB version change (configuration or interface).
771302	Spoke cannot register to OCVPN when FortiGate is in policy-based NGFW mode.

Log & Report

Bug ID	Description
621329	Mixed traffic and UTM logs are in the event log file because the current `category` in the log packet header is not big enough.
745689	Unknown interface is shown in flow-based UTM logs.
747854	PDF report generation fails due to an HPDF API error when it is drawing a circle and there is only one entry in the SQL result.
749440	IPS malicious URL database (idsurldb, MUDB) update entry in `FortiGate update succeeded` log is delayed from the actual update timing.
749842	The miglogd process uses high CPU when handling a web rating error log that is reported with an invalid VDOM ID.
751358	Unable to set source IP for FortiCloud unless FortiCloud is already activated.
753904	The reportd process consumes a high amount of CPU.
754143	Add `srcreputation` and `dstreputation` fields in the forward traffic logs to provide the reputation level of the source and destination when the traffic matches an entry in the internet service database.
757703	Report suddenly cannot be generated due to no response from reportd.

Proxy

Bug ID	Description
568905	WAD crashes due to RCX having a null value.
712584	WAD memory leak causes device to go into conserve mode.
723764	Replacement page is not provided to client when blocking traffic from an application control profile.
729797	CLI should block or warn users if an API gateway with the same service (protocol) and path are declared on the same ZTNA server.
733135, 734840	Web filter is blocking websites in proxy mode due to SSL certificate validation failure, which is caused by an unreachable OCSP server.
738151	Browser has *ERR_SSL_KEY_USAGE_INCOMPATIBLE* error when both ZTNA and web proxy are enabled.
739627	`diagnose wad stats policy list` does not show statistics correctly when enabling certificate inspection and HTTP policy redirect.
743746	WAD encounters signal 11 crash when adding user information.
746796	Stream-based scanning has high CPU cost and a long wait time on GZIP and BZIP2 files.
747250	When a timeout happens while forticron is downloading a file, the original downloaded file is not be deleted, so the next successful download has extra data in front.
751674	Load balancer based on HTTP host is DNATing traffic to the wrong real server when the correct real server is disabled.
752744	Proxy-based certificate with deep inspection fails upon receipt of a large handshake message.
754298	WAD crashes when adding user information.
754969	Explicit FTP proxy chooses random destination port when the FTP client initiates an FTP session without using the default port.
755294	Firefox gives `SEC_ERROR_REUSED_ISSUER_AND_SERIAL` error when ECDSA CA is configured for deep inspection.
755685	Trend Micro client results in FortiGate illegal parameter SSL alert response because the Trend Micro client sent a ClientHello that includes extra data, which is declined by the FortiGate according to RFC 5246 7.4.1.2.
756603	WAD memory spike when downloading files larger than 4 GB.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
756887	WAD crashes if the certificate authentication request context is not closed in the following scenarios: when fnbamd returns a failure certificate authentication result or no response; and when the CA certificate is updated and the certificate cache is flushed.
757873	WAD crash in half-mode virtual server case and HTTP real server ZTNA case.

Bug ID	Description
758122	WAD memory usage may spike and cause the FortiGate to enter conserve mode when downloading a large file fails.
758496	WAD crash for LDAP group looping.
758532	WAD memory usage may spike and cause the FortiGate to enter conserve mode.
764193	The three-way handshake packet that was marked as `TCP port number reused` cannot pass through the FortiGate, and the FortiGate relies with a `FIN, ACK` to the client.
765349	Once AV is enabled in proxy mode, traffic will be blocked in proxy mode.
768358	Failure to access certain AWS pages with proxy SSL deep inspection.

REST API

Bug ID	Description
743169	Update various REST API endpoints to prevent information in other VDOMs from being leaked.
768056	HTTPS daemon is not responsive when successive API calls are made to create an interface.

Routing

Bug ID	Description
720320	OSPF issues with spokes randomly showing `Process is not up` and losing some routes.
731941	`Disconnected from FortiAnalyzer` events reported when the `interface-select-method` is set to `specify`, and the `interface port_<x>` is set to an interface that does not have the highest priority in the SD-WAN interface selection.
745999	Routing issue occurs when one of the SD-WAN interfaces goes down.
748733	Remote IP route shows `incomplete inactive` in the routing table, which causes issues with BGP routes where the peer is the next hop.
762258	When policy-based routing uses a PPPoE interface, the policy route order changes after rebooting and when the link is up/down.
754636	Traffic sometimes does not match SD-WAN rules on some IPsec interfaces.
759711	OSPF E2 routes learned by Cisco routers are randomly removed from the routing table when the OSPF/OSPFv3 neighbor flaps.
759752	FortiGate is sending malformed packets causing a BGP IPv6 peering flap when there is a large amount of IPv6 routes, and they cannot fit in one packet.

Security Fabric

Bug ID	Description
748389	Security Fabric automation email action trigger shows multiple emails as one email with no separation between the addresses.
753056	Recommendation information for *Failed Login Attempts* security rating rule should display *Lockout duration should be at least 30 minutes*, instead of 1800 minutes.
755187	The security rating test for *Unused Policies* is incorrectly evaluated as *Pass* when there are unused policies with the accept action.
758493	SDN connector on FG-Azure stays stuck if it is alphabetically the first subscription that is not in the permission scope.
765525	The deleted auto-scripts are not sent to FortiManager through the auto-update and cause devices go out of sync.

SSL VPN

Bug ID	Description
673320	Pop-up window does not load correctly when accessing internal application at https://re***.wo***.nl using SSL VPN web mode.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
684010	Internal page, https://vpn.ea***.***.**.us:10443, is not working in SSL VPN web mode.
695457	JS error thrown when accessing HTTPS bookmark (mk***.ag***.cp***.vw***) using SSL VPN web portal.
722329	After SSL VPN proxy rewrite, some Nuage JS files have problems running.
737894	If there are no users or groups in an SSL VPN policy, the SSL VPN daemon may crash when an FQDN is a destination address in the firewall policy.
746938	Unable to authenticate to outlook.com/owa/vw***.com website in SSL VPN web mode.
748085	SSL VPN authentication is not working for RADIUS users because the LDAP responds first.
748660	Unable to access Apache Guacamole web application using SSL VPN web mode.
749452	SSL VPN login authentication times out if primary RADIUS server becomes unavailable.
749815	Unable to access webmail server (https://9**.1**.9**.2**/) using SSL VPN web mode.
751028	SSL VPN proxy error in web mode for https://et***.ga***.gov.***/ due to requests to the loopback IP.
751366	JS error in SSL VPN web mode when trying to retrieve a PDF from https://vpn.ca***.com/.
751643	Jira server (cb***.com.au) cannot be displayed correctly using SSL VPN web mode.

Bug ID	Description
751697	SSO login for SSL VPN bookmarks (https://za***.jo.za***.com) is not working.
751717	SAML user configured in groups in the IdP server might match to the wrong group in SSL VPN user authentication if an external browser is used.
752055	VNC (protocol version 3.6/3.3) connection is not working in SSL VPN web mode.
753515	DTLS does not work for SSL VPN and switches to TLS.
753590	Brickstream web interface is not loading properly when accessed using SSL VPN webmode.
755296	SSL VPN web mode has issues accessing https://e***.or***.kr.
756753	FQDN in firewall policy is treated case sensitive, which causes SSL VPN failure when redirecting or accessing a URL that contains capitalized characters.
758525	Users can modify the URL in SSL VPN portal to show connection launcher even when the *Show Connection Launcher* option is disabled.
759664	Renaming the server entry configuration will break the connection between the IdP and FortiGate, which causes the SAML login for SSL VPN to not work as expected.
760340	WebSocket using Pronto Xi could not be established through SSL VPN web mode.
760928	SSL VPN with RADIUS authentication does not work with an interface subnet address object.
761668	Empty webpage loads when accessing internal website, https://ba***.ba**.com:2222, in SSL VPN web mode.
762491	Unable to authenticate outlook.office.com using corporate domain email account.
763619	SAP Fiori webpage using JSON is not loading in SSL VPN web mode.
767869	SCADA portal will not fully load with SSL VPN web bookmark.
768994	SSL VPN crashed when closing web mode RDP after upgrading.
771145	SSL VPN web mode access problem occurs for web service security camera.
773254	SSL VPN web mode access is causing issues with MiniCAU.

Switch Controller

Bug ID	Description
740661	FortiGate loses FortiSwitch management access due to excessive configuration pushes.
766583	A bin/cu_acd crash is generated when `cfg-revert` is enabled and involves FortiSwitch.

System

Bug ID	Description
572847	The wan1, wan2, and dmz interfaces should not be configured as hardware switch members on the 60F series. The wan interface should not be configured as a hardware switch member on the 40F series.
596942	SoC3 platforms may encounter kernel panic in cases when a PKCE IOCTL wait event is interrupted by WAD diagnose CLI commands.
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.
643558	System halts after running `execute update-now` in FIPS-CC mode.
651626	A session clash is caused by the same NAT port. It happens when many sessions are created at the same time and they get the same NAT port due to the wrong port seed value.
671116	Lack of null pointer check in NP6XLite driver may lead to kernel panic. Affected models: FG-40F, FG-60F, and FG-101F.
675558	SFP port with 1G copper SFP always is up.
679035	NP6 drops, and bandwidth is limited to under 10 Gbps in `npu-vlink` case.
683299	Port group members have different speeds after the port speed is changed using a CLI script.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
703219	Kernel panic on FG-101F due to lack of null pointer check on NP6XLite driver.
712156	Remote access management from FortiCloud login fails if trusted hosts are configured for the administrator account.
712258	SFP28 ports on FG-340xE/FG-360xE cannot receive or transmit packets when the speed is set to 1000full. This issue is triggered by warm rebooting the FortiGate/Cisco switch or disconnecting the fiber cable.
716341	SFP28 port flapping when the speed is set to 10G.
718307, 729078	Verizon LTE connection is not stable, and the connection may drop after a few hours.
720687	On FG-20xF, the RJ45 ports connected to Dell N1548 switch do not automatically have an up link for energy detect mode.
726705	After upgrading to 7.0.0, FG-60E hangs due to various CLI configuration errors starting with `cli 102 die in an exception in line 4318: KV?.`
738640	There is no I2C reading/writing handler in drivers for FGR-60F and FGR-60F-3G4G.
741359	As per IEEE 802.3, NP frames under 64 octets should be discarded on the RX.
741944	The forticron process has a memory leak if there are duplicated entries in the external IP range file.

Bug ID	Description
744892	DNS query responses can be bumped when dealing with a high volume of visibility hostname log requests.
749250	Firewall does not use its ARP cache and is ARPing for client MAC addresses every 20 to 30 seconds.
749613	Unable to save configuration changes and get `failed: No space left on device` error.
749835	Traffic logs report ICMP destination as unreachable for received traffic.
750123	FG-100F/101F sensor list shows the following deficiencies: missing PSU reading, degree sign is not readable in some CLI windows, and spelling mistakes.
750171	Legitimate traffic is unable to go through with NP6 `synproxy` enabled.
750202	USB unmounts after configuration backup.
751227	The GA image becomes uncertified after backing it up on a flash disk.
751346	DNS server obtained via DHCPv6 prefix delegation is not used by DNS proxy.
751523	When changing mode from DHCP to static, the existing DHCP IP is kept so no CLI command is generated and sent to FortiManager.
753421	Slow SNMP query performance of fgVpn2Tables OIDs when a large number of IPsec dialup tunnels are connected.
753602	FG-40F has a newcli signal 11 crash.
753862	DHCPc seconds not incrementing in DHCP DISCOVER, REQUEST, and INFORM packets.
754567	FortiGate receives `Firmware image without valid RSA signature loaded` error when loading the image from FortiCloud.
754951	Static ARP entry was removed while using DHCP relay.
755475	When a software switch has an intra-switch-policy set to implicit (the default setting), layer 2 traffic, such as LLDP or STP, is being forwarded when it should be denied by default.
755953	Direct CLI script from FortiManager fails due to additional `end` at the end of `diagnose debug crashlog read`.
756160	Unable to configure firewall access control lists on FG-20xF.
756445	Flow-based inspection on WCCP (L2 forwarding) enabled policy with VLAN interfaces causes traffic to drop if `asic-offload` is enabled.
756713	Packet Loss on the LAG interface (eight ports) in static mode. Affected models: FG-110xE, FG-220xE, and FG-330xE.
757689	When creating a new interface with MTU override enabled, PPPoE mode, and a set MTU value, the MTU value is overridden by the default value.
757733	CP9 or SoC3/SoC4 kernel driver may crash while doing AES-GCM decryption.
757748	WAD memory leak could cause system to halt and print `fork() failed` on the console.

Bug ID	Description
758545	Memory leak cause by leaked JSON object.
758815	Connectivity issue on port26 because NP6 table configuration has an incorrect member list. Affected models: FG-110xE, FG-220xE, and FG-330xE.
760259	Outbound bandwidth in bandwidth widget does not adhere to the outbandwidth setting.
764989	Include an entry in SNMP OID that lists the number of octets for the IP type.

Upgrade

Bug ID	Description
743389	The `dnsfilter-profile` setting was purged from all DNS server entries upon upgrading from below 6.4.4.
744454	IPv6 delegated configuration is lost after upgrading from 7.0.1.

User & Authentication

Bug ID	Description
709964	Apple devices cannot load the FortiAuthenticator captive portal via the system pop-up only.
719658	SCEP client does not work with virtual service.
739350	RADIUS response is sent even when the `rsso-radius-response` attribute is set to `disable`.
742244	Unable to receive token via email on configured local email server with authentication when the incoming SMTP response is incomplete.
747651	There is no LDAP-based authentication possible during the time WAD updates/reads group information from the AD LDAP server.
750551	DST_Root_CA_X3 certificate is expired.
753449	SCEP using `execute vpn certificate local generate` does not conform to HTTP 1.1 RFC 2616.
755302	The fnbamd process spikes to 99% or crashes during RADIUS authentication.
756763	In the email collection captive portal, a user can click *Continue* without selecting the checkbox to accept the terms and disclaimer agreement.
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.

VM

Bug ID	Description
691337	When upgrading from 6.4.7 to 7.0.2, GCP SDN connector entries that have a `gcp-project-list` configuration will be lost.
747221	Tags under VNET are not detected by SDN connector under Azure. The following issues have been fixed: • IP of Azure network interface without an associated VM is not collected. • Address prefix of Azure subnet is not collected. • Tags on Azure virtual network scope cannot filter the IP address.
750889	DHCP relay fails when VMs on different VLAN interfaces use the same transaction ID.
755016	In AWS, if the HA connection between active and passive nodes breaks for a few seconds and reconnects, sometimes the EIP will remain in the passive node.
759300	gcpd has signal 11 crash at `gcpd_mime_part_end`.
764184	Inconsistent TXQ selection degrades mlx5 vfNIC. Azure FortiGate interface has high latency when the IPsec tunnel is up.
769352	Azure SDN connector is unable to pull service tag from China and Germany regions.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).

WAN Optimization

Bug ID	Description
754378	When an AV profile is enabled in a WANOpt proxy policy on a server side FortiGate, EICAR sent over HTTPS will not get blocked.

Web Filter

Bug ID	Description
751693	WAD crashed with signal 6 when using WIPS for web filtering with Websense.

WiFi Controller

Bug ID	Description
578440	Wireless controller sends ARP request packets that are destined to the FortiGate back to all tunnel interfaces.
600257	FG-1000D and FG-1500D go in to conserve mode when wpad and cw_acd have a memory spike, which affects wireless user tunnel traffic.
675164	FWF-60F local radio shows WPA3 is not supported.
720497	MAC authentication bypass is not working for some clients
734801	Some Apple devices cannot handle 303/307 messages, and may loop to load the external portal page and fail to pass authentication. Some android devices cannot process JavaScript redirect messages after users submit their username and password.
744687	Client should match the new NAC policy if it is reordered to the top one.
745044	Optimize memory usage of wpad daemon in WiFi controller for large-scale 802.11r fast BSS transition deployment.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.
751509	On FAP-U432F, the *Radio 3* spectrum analysis should be disabled in the FortiGate GUI.
761996	If `concurrent-client-limit-type` is set to `unlimited` it is limited by the `max-clients` value in the VAP profile.
766652	FortiAP firmware status is inconsistent on *System* > *Fabric Management* page and upgrade slide.

ZTNA

Bug ID	Description
765813	ZTNA access is systematically denied for ZTNA rule using SD-WAN zone as an incoming interface.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
752134	FortiOS 7.0.4 is no longer vulnerable to the following CVE Reference: • CVE-2021-42757
752450	FortiOS 7.0.4 is no longer vulnerable to the following CVE Reference: • CVE-2021-44168

Known issues

The following issues have been identified in version 7.0.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Firewall

Bug ID	Description
719311	FortiGate shows partial view of policies after upgrading.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page, when VDOM mode is enabled, the *Global* view shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.

Bug ID	Description
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
713529	When FortiAnalyzer is configured, the HTTPS daemon may crash while processing some FortiAnalyzer log requests. There is no apparent impact on the GUI operation.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
771389	SNMP community name with one extra character at the end stills matches when HA is enabled.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.

Proxy

Bug ID	Description
692444	WAD memory leak is caused by missing a close event. The WAD receives a close event from TCP when the SSL port is blocked by the up application layer. If the SSL port input buffer does not have any data, then the close event will get ignored even if the application layer turns off blocking and the SSL port will leak.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.

System

Bug ID	Description
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.

VM

Bug ID	Description
689047	ARM64-KVM has kernel panic.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used.

Bug ID	Description
	Workaround: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`.

WiFi Controller

Bug ID	Description
750425	In RADIUS MAC authentication, the FortiGate NAS-IP-Address will revert to `0.0.0.0` after using the FortiGate address.

Built-in AV engine

Resolved engine issues

Bug ID	Description
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com